PATENT SPECIFICATION (11) 1 595 797

1 595 797

(21) Application No. 17128/80 (22) Filed 21 April 1978

(62) Divided out of No. 1 595 796

(44) Complete Specification published 19 Aug. 1981

(51) INT. CL.³ E05B 47/00

(52) Index at acceptance
G4H 13D 14A 1A TG

(54) SECURITY SYSTEMS.

(71) I, HUGH JOHN PUSHMAN, of British Nationality, of 63 Woolaton Road, Ferndown, Dorset, do hereby declare the invention for which I pray that a patent may be granted to me, and the method by which it is to be performed, to be particularly described in and by the following statement:

This invention relates to security systems.

According to the invention, a security system comprising a key and, separate from the key, a control means for actuation by the key, the key comprising a first generator of a pseudo-random sequence of signals, and the control means being capable of receiving said signals and comprising a second generator of the same pseudo-random sequence of signals as the first generator and comparison means operative to compare a received signal sequence with the signal sequence generated by the second generator and responsive to complete correlation between at least part of the two sequences to develop a control signal to effect a control function, wherein the first generator comprises a first shift register and a first logic circuit connected to receive the contents of at least one stage of the first shift register, the first logic circuit having an output which is connected back to a stage of the first shift register, the second generator comprises a second shift register and a second logic circuit connected to receive the contents of at least one stage of the second shift register, the control means is so designed that a received signal sequence is directed to a stage of the second shift register corresponding to that stage of the first shift register to which the output of the first logic circuit is connected, and the comparison means comprises a comparator having a first input connected to receive a received signal sequence and a second input connected to the output of the second logic circuit.

The system may be such that the key has to be positioned in contact with the control means to actuate it. For example, the signals provided by the key could be electrical and the key control means could be provided with cooperating contacts. The system may instead be such that the key can be disposed remote from the control means to actuate it, e.g. it may be connected thereto by a communication link, e.g. a telephone circuit, or by radiation, e.g. light (visible or invisible), other electro-magnetic radiation or acoustic radiation.

Although in many systems embodying the invention the key will, like the key of a conventional mechanical lock, be manually portable, it is not necessarily so. For example, if a system in accordance with the invention is used for locking and/or unlocking a garage door, the key could be embodied in a vehicle and be arranged to generate the signal sequence by flashing the headlights thereof, for instance by means of a mechanical timer switch, the control means being light-sensitive and being associated with the garage door lock.

As just mentioned, the application of systems in accordance with the invention is to the opening and closing of locks, in which case the control means is associated with the lock. For instance, the control means can be incorporated in a safe. However, other applications of the system are possible.

Naturally, the control means of a system embodying the invention can only be actuated by a key having a generator providing the same sequence of signals as that provided by the generator of the control means. To provide additional security, the code of the sequence generated by the generator of the control means can be altered, for example, at regular or irregular intervals or upon use. The code of the key generator sequence could be similarly variable, whereby the user would have to set the appropriate code on the key before it could actuate the control means.

A further advantage of a key having provision for varying the code of the

sequence manually is that it can only be used to operate an associated control means by a person knowing the correct code setting.

The invention will now be further described, by way of example, with reference to the accompanying drawing, in which:

Figure 1 is a schematic diagram of a pseudo-random pulse generator that can be employed in the key of a system embodying the invention; and

Figure 2 is a block diagram of the system embodying the invention.

Referring first to Figure 1, the pseudo-random generator shown therein comprises an n-stage shift register 10. A clock pulse generator (not shown) supplies pulses to the shift register 10 to shift its contents from left to right as shown in the drawing. The r^{th} and s^{th} stages of the shift register are connected to inputs of a logic circuit 12, which may be exclusive-OR gate or a "2's complement" circuit. The output from the logic circuit 12 is connected back to the first stage 1 of the shift register. When clock pulses are supplied to the shift register 10, by virtue of the logic circuit 12 a pseudo-random output sequence of a predetermined number of bits will be generated at the output of the logic circuit 12. The output is not truly random in that if all relevant factors are known its form can be accurately predicted. However, each bit in the sequence bears little or no correlation to adjacent ones so that for practical purposes the output can be considered random.

The nature of the sequence is dependent upon the initial state of the shift register 10, the number of stages of the shift register 10, the logical operation carried out by the logic circuit 12 (other operations than an exclusive-OR operation can be carried out), and the stage tappings employed (the logic circuit 12 can be connected to different stages and not necessarily to two stages).

A further relevant factor is that the code produced may or may not be 'optimum'. An optimum code is defined as one where the code adopts all possible states before repeating itself. For example, a 16 stage register can produce a code 2^{16} bits long before repeating itself. A non-optimum code is defined as one where the sequence stops short of the maximum possible figure. For example, a 16 bit register may be arranged to produce codes of 48 K bits and 16 K bits or of 16 K, 32 K and 16 K bits. Whether the code is optimum or not is determined by the stages connected to the logic circuit 12 and the nature of the logical operation it carries out. If the code is not optimum, the code cycle is determined by the initial state of the register.

The mathematical theory of pseudo-random generators as described above is well-developed, and the characteristics of the sequences they produce can be analysed and forecast.

A security system shown in Figure 2 comprises a key 20 and control means 30. The key 20 comprises a pseudo-random generator which is of the form described with reference to Figure 1 and comprises a shift register 10 and a logic circuit 12 connected as described with reference to Figure 1.

If appropriate, the key 20 may be provided with a transducer which converts the electric pseudo-random output sequence from the pseudo-random generator into, for example, electromagnetic radiation for transmission to the control means 30. In this case, the control means 30 will be provided with a transducer responsive to radiation received from the key 20 to convert it back into electrical signals. The operative connection between the key 20 and control means 30 can in fact be effected in a variety of ways. For instance, if light is used, the key transducer could be a light emitting diode (LED) and the light could either be shone through space on to the control means 30 or conducted thereto by means of an optical fibre. Naturally, if the connection between the key 20 and control means is electrical, the transducers are not needed.

The control means 30 comprises a pseudo-random generator constituted by a shift register 10′ and a logic circuit 12′. The generator in the control means is identical to that in the key 20 except that the output of the logic circuit 12′ is not connected back to the first stage of the shift register 10′. Instead, the pseudo-random signal sequence from the key 20 is supplied to the first stage of the shift register 10′. The control means 30 further comprises a comparator 32, which may be a half-adder, which has a pair of inputs of which one is connected to receive the pseudo-random signal sequence from the key 20 and the other is connected to the output of the logic circuit 12′. The output 34 of the comparator 32 constitutes the output of the control means 30.

The security system of Figure 2 operates as follows. The pseudo-random signal sequence from the key 20 is fed into the shift register 10′ of the pseudo-random generator of the control means 30. Since the two pseudo-random generators are of identical construction, after a delay equal to the time taken for the pseudo-random signal to be transferred the length of the

shift register 10′ the signals supplied to the two inputs of the comparator 32 will be in synchronism and identical. Accordingly, the comparator will in response thereto produce on the output 34 a control signal for effecting a control function, e.g. to actuate a lock.

To provide additional security, the system described above can be elaborated in a variety of ways. For instance, the coding of the sequence generated by the pseudo-random generator of the control means 30 could be varied from time to time as described hereinabove with reference to Figure 1, for instance by providing a multi-position switch between the shift register 10′ and the logic circuit 12′ to change the stage tappings i.e. to change the number of tappings and/or the particular tappings connected to the logic circuit. The code could be changed at fixed or random intervals (e.g. by means of an internal timer) or could be changed automatically after each occasion of use. The setting of the code generated by the pseudo-random generator of the key will be similarly variable, and the user would have to know the correct setting to be able to actuate the control means. In this way, additional security similar to that provided by a combination lock could be obtained.

It is possible to manually vary the key code, for example by means of a keyboard provided on the key. Manual code variations can be superimposed on the output of the code generator.

As will be appreciated, provision on the key of means for manually setting an appropriate code has the advantage that loss or theft of the key does not in itself mean that the finder or thief can operate the control means without hindrance. The possibility of the code being changed from time to time or by use means that the keyholder himself may not be able to use the key until he has obtained information as to the correct setting from an alternative or remote source. This facility could help prevent a key being used by the holder under duress, for instance under threat to himself or to hostages

It is possible for the key to be fabricated in two or more parts, whereby two or more persons will be needed to actuate the control means. It is further possible to arrange that variations of the set code from an appropriate setting will allow actuation of the control means, but will cause a hidden or silent alarm to be actuated.

Operation of the control means from a completely remote location, e.g. via a telephone line, is feasible.

A system in accordance with the invention could be used to safeguard the transportation of valuables. For instance, a container and/or vehicle provided with a control means in accordance with the invention and with the key not carried on the vehicle couldl not be unlocked until its destination has been confirmed and cleared.

In the system described above with reference to the drawing, no signal for synchronising the codes of the key and control means is needed and a high degree of security is provided.

The system of Figure 2 could be modified by including in the key 20 means to modulate (e.g. phase modulate) a further signal (e.g. a digital signal) with the pseudo-random signal sequence of the key generator and including in the control means 30 means to demodulate the received modulated signal prior to applying it to the comparator 32 and the shift register 10′. The modulation technique employed can in fact comprise so-called bi-phase-mark encoding as described in the complete specification of my copending UK Patent Application No. 8826/77 (Serial No. 1595796), from which the present application was divided out and to which reference should be made.

The circuits disclosed above are suitable for embodiment in LSI form, e.g. one chip each for the key and control means. Each chip may comprise, for example, a programmable ROM, whereby a desired coding for the pseudo-random generator can be 'burnt-in'.

WHAT WE CLAIM IS:—

1. A security system comprising a key and, separate from the key, a control means for actuation by the key, the key comprising a first generator of a pseudo-random sequence of signals, and the control means being capable of receiving said signals and comprising a second generator of the same pseudo-random sequence of signals as the first generator and comparison means operative to compare a received signal sequence with the signal sequence generated by the second generator and responsive to complete correlation between at least part of the two sequences to develop a control signal to effect a control function, wherein the first generator comprises a first shift register first generator comprises a first shift register and a first logic circuit connected to receive the contents of at least one stage of the first shift register, the first logic circuit having an output which is connected back to a stage of the first shift register, the second generator comprises a second shift register and a second logic circuit connected to receive the contents of at least one stage of the

second shift register, the control means is so designed that a received signal sequence is directed to a stage of the second shift register corresponding to that stage of the first shift register to which the output of the first logic circuit is connected, and the comparison means comprises a comparator having a first input connected to receive a received signal sequence and a second input connected to the output of the second logic circuit.

2. A security system according to claim 1, wherein each of the first and second logic circuits is an exclusive-OR gate.

3. A security system according to claim 1 or claim 2, including, in each generator, switch means connected between the shift register and the logic circuit and operable to enable variation of the number of stages and/or the stages of the shift register to which the logic circuit is connected to cause variation of the pseudo-random signal sequence.

4. A security system according to claim 3, wherein the switch means of the first generator is manually operable and the switch means of the second generator is automatically operable.

5. A security system according to claim 4, wherein the control means includes a timer operative on the switch means thereof to periodically alter the pseudo-random signal sequence.

6. A security system according to any one of the preceding claims wherein the key includes means to modulate a further signal with the pseudo-random signal sequence of the first generator and the control means includes means to demodulate the received modulated signal prior to applying it to the comparison means and the second shift register.

7. A security system according to claim 6, wherein the means to modulate and the means to demodulate provide angle modulation and demodulation, respectively, of the further signal.

8. A security system according to claim 7, wherein the means to modulate and the means to demodulate provide phase modulation and demodulation, respectively, of the further signal.

9. A security system according to any one of claims 6, 7 and 8, wherein said further signal is a digital signal.

10. A security system according to any one of claims 1 to 9, wherein the pseudo-random signal sequences are in electrical form, the key comprises a transducer to convert the pseudo-random signal sequence into non-electrical form for transmission to the control means, and the control means comprises a transducer to reconvert a received pseudo-random signal sequence to electrical form prior to its application to the comparison means.

11. A security system according to claim 10, wherein the key transducer is operative to convert the pseudo-random signal sequence into a luminous (visilbe or invisible) form.

12. A security system according to claim 11, wherein the key transducer is a light emitting diode.

13. A security system according to claim 11 or claim 12, including light guide means for transmitting the luminous signal sequence from the key to the control means.

14. A security system according to claim 13, wherein the light guide means comprises fibre optics light guide means.

15. A security system according to any one of claims 1 to 9, wherein the pseudo-random signal sequences are in electrical form and the key and control means are so constructed that the key can supply its signal sequence to the control means by direct electrical connection of the key and control means.

16. A security system according to any one of claims 1 to 9, wherein the pseudo-random signal sequences are in electrical form, the system comprising a communications link to transmit the pseudo-random signal sequence of the first generator from the key to the control means.

17. A security system according to claim 16, wherein the communications link is a telephone circuit.

18. A security system according to claim 16, wherein the communications link is a radio link.

19. A security system substantially as herein described with reference to the accompanying drawing.

For the Applicant:
D. YOUNG & CO.,
Chartered Patent Agents,
10 Staple Inn,
London WC1V 7RD.

Printed for Her Majesty's Stationery Office by The Tweeddale Press Ltd., Berwick-upon-Tweed, 1981.
Published at the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

1595797 COMPLETE SPECIFICATION
1 SHEET This drawing is a reproduction of the Original on a reduced scale

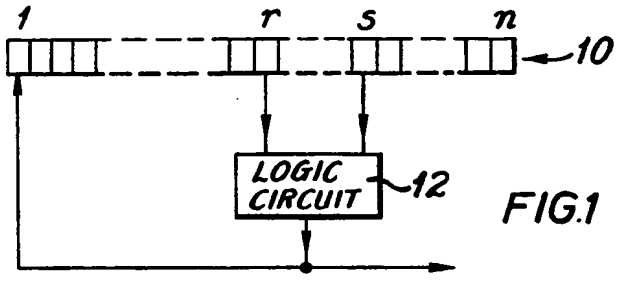

FIG.1

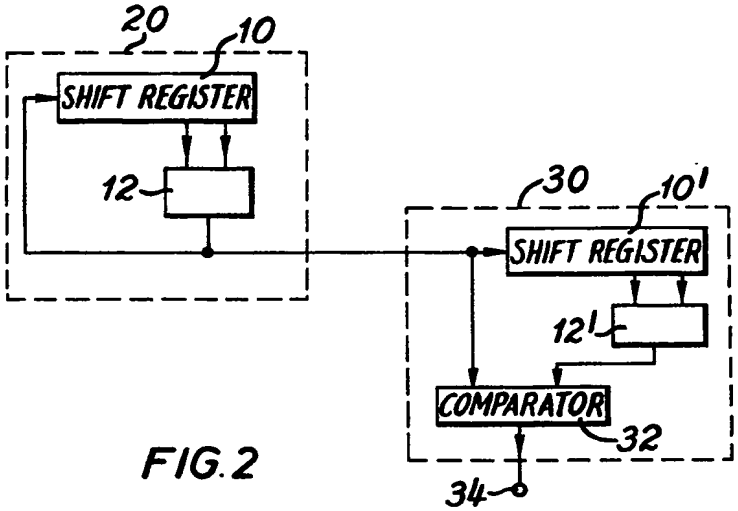

FIG.2